Deux grands défis du RGPD : comment les relever ?

Auteur et fonction : Judith Duchêne, Conseillère

Le 25 mai 2018… nous y sommes, nous y voilà ! Le RGPD fait désormais partie de votre quotidien, et toutes les questions qui sont au cœur de votre métier en CPAS en sont teintées. Suite au colloque qu'elle a organisé le 27 mars dernier à ce sujet, la Fédération des CPAS continue à vous informer : un article[1] reprenant 4 questions essentielles liées à son application a été publié dans le CPAS Plus de mai, ainsi que sur notre site internet[2].

En reprenant un peu de hauteur, cet article vise à souligner deux grands défis de l'opérationnalisation du RGPD. Il nous semble nécessaire de les mettre en exergue afin de les poser comme un horizon à garder à l'esprit dans chaque action concrète que vous prendrez pour la mise en conformité. Car, ce qui importe fondamentalement, c'est bien que les démarches et les outils concrétisés dans le cadre du RGPD viennent consolider l'exercice de votre métier.

La rédaction de cet article est basée sur l'intervention de Dominique Grégoire[3] lors de notre journée d'information.

1. *Privacy by design* et *privacy by default*

Globalement, la mise en conformité au RGPD est présentée comme un défi où il n'y aurait que des procédures à appliquer (un registre à mettre en place, des analyses d'impact à faire, …).

Ces procédures permettant de connaître les traitements réalisés par l'institution et l'analyse de gestion des risques sont en fait plutôt à considérer comme des balises permettant de garantir les étapes de mise en application de ce qui est attendu sur le fond ; à savoir, que l'organisation fasse du « privacy by default et by design ».

Le « privacy by design » est le fait que le responsable de traitement doit penser à la sécurité de celui-ci dès qu'il envisage un traitement de données, Ainsi que dans toutes les étapes de sa mise en œuvre.

Le « privacy by default » est le fait que, par défaut, la personne dont les données sont traitées bénéficie du niveau maximal de protection.

Pour parvenir à relever ces deux grands défis, il est nécessaire d'intégrer, dans toute l'organisation et dans tous ses process, les mesures de protection qui concernent la vie privée.

---

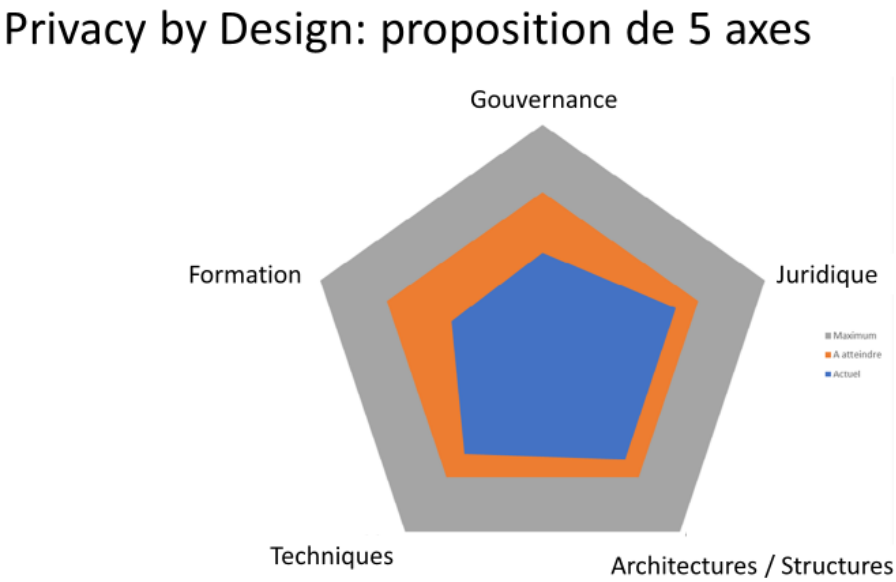
[1] J. Duchêne, *RGPD : 4 questions avant le 25 mai 2018*, *CPAS Plus*, 5/2018.
[2] Voir le lien suivant : http://www.uvcw.be/no_index/cpas/actions/369-137994722165050320180306018005108680 28.pdf
[3] Conseiller en sécurité de l'information (FOREM) et Président du Groupe de travail sur la sécurité de l'information (GTSI).

Pour ce faire, il est important de créer un environnement culturel, managérial, technologique et réglementaire. L'organisation doit donc se transformer et gagner en maturité afin de créer un environnement propice à la protection des données.

Cette transformation est essentielle pour assurer la conformité au règlement dans la continuité. En effet, par exemple, réaliser un registre de traitement pour le 25 mai 2018, sans prévoir les procédures organisationnelles nécessaires le maintenir à jour serait un travail vain.

Dans cette démarche, tous les niveaux de l'organisation doivent être concernés :

- Micro : informatique – techniques de sécurité
- Meso : procédures techniques et organisationnelles à mettre en place
- Macro : gouvernance, formation, dimensions juridiques transversales dans l'organisation



Pour initier une telle démarche, la pertinence des données par rapport au métier doit être interrogée : comment utilise-t-on les données ? Où sont-elles stockées ? Qui en a besoin ? Comment peuvent-elles être optimisées ?

Il s'agit de mettre la donnée au centre de la réflexion, et donc de transformer l'organisation afin de mettre en œuvre une véritable *Gouvernance des Données*. De la sorte, les dimensions relatives à la protection et la sécurité des données peuvent être intégrées de manière totalement transparente et quasiment sans surcoût dans chaque projet.

Une personne seule ne peut pas parvenir à opérer cette transformation. C'est pourquoi il est essentiel de sensibiliser et de former tous les acteurs afin de multiplier les relais au sein de l'organisation et que les réflexes relatifs à la protection des données puissent se diffuser.

Le DPD peut jouer ce rôle : un rôle de conseiller, de facilitateur qui va faciliter l'émergence d'une telle culture au sein de l'organisation.

Dans le contexte mouvant des organisations, une approche du changement systémique et par émergence - qui s'appuie notamment sur l'autonomisation des acteurs et une adaptation permanente au contexte – est bien souvent plus pertinente et pragmatique qu'une approche planificatrice classique. En effet, opérer un changement organisationnel d'une telle importance par une logique où tout est planifié longtemps à l'avance, dans une organisation qui change très fort, dans un contexte politique qui change très fort, dans une société qui change très fort, n'aboutit généralement pas au résultat escompté ou produit en fin de compte un résultat qui n'est pas compatible avec le nouveau contexte.

Dans l'approche systémique et par émergence, plutôt que de vouloir tout contrôler, le DPD cherche des relais, il les forme, il les autonomise, il les sensibilise à la sécurité. Il laisse à chacun le choix de ses outils, en fonction de son expertise et de son domaine de compétence.

Cette approche par émergence se situe moins dans une logique de maîtrise/de contrôle que de confiance. Elle reconnaît que la personne qui est au plus près de la donnée est en capacité de la maîtriser au mieux, parce qu'elle connaît son contexte d'utilisation. Elle fait en sorte que chaque personne, à chaque niveau, commence réellement à se préoccuper de la protection des données. Elle rend le terreau fertile pour que les principes-clés du RGPD puissent y trouver de la consistance et perdurer dans le temps, car la protection des données et de la vie privée n'est plus le fruit d'une application forcée de procédures et de règles, mais de valeurs intégrées dans le cœur de l'organisation.

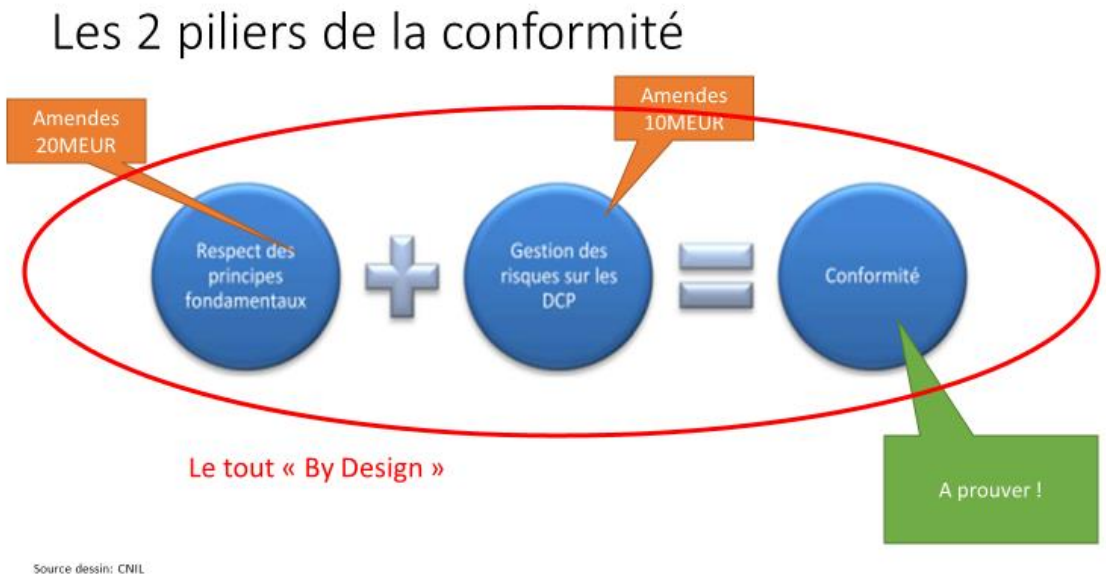
2. Accountability

Un des grands changements du RGPD par rapport à la loi vie privée[4] réside dans cette notion d' « accountability ». Le responsable de traitement doit pouvoir prouver qu'il respecte bien le règlement.

Que doit-il prouver ?

- Qu'il a bien fait les choses (qu'il n'a pas triché)
- Qu'il a suffisamment bien fait les choses, qu'il est arrivé à un niveau suffisant de protection des données.

[4] L. 8.12.1992 rel. à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B. 18.3.1993.



Le RGPD met en avant deux perspectives : des critères que l'on pourrait qualifier d'*objectifs* (ex. : registre de traitement et analyse d'impact) et des critères *subjectifs* (ex. : protection des données elles-mêmes et mesures de sécurité mises en place).

La conformité aux critères objectifs est la plus facile à atteindre. De ce point de vue, les organisations ont intérêt à s'y conformer au plus vite, car c'est probablement aussi sur ces critères objectifs que le contrôle est le plus facile à effectuer.

La rencontre des critères subjectifs va être dépendante de l'efficacité des mesures de sécurité mises en place et du contexte organisationnel. Cette efficacité sera inévitablement comparée à des « bonnes pratiques », des normes telles que les normes ISO ou les normes minimales de la BCSS. Il est donc important de s'en inspirer afin de plus facilement prouver la pertinence des mesures mises en œuvre.

Pour être conforme, il faut, d'une part, respecter les principes fondamentaux du règlement[5] et, d'autre part, mettre en œuvre une gestion des risques sur les données à caractère personnel. Il faut en outre le prouver, en documentant et en justifiant, les traitements, les risques et les mesures de protection.

Très souvent, en pratique, tout ne pourra pas être fait en une fois ; mais avec les moyens qui sont à disposition, il faut pouvoir mettre tout en place pour faire au mieux. Une approche pragmatique, qui mise sur des fondations solides visant à construire du « privacy by design » au niveau structurel et organisationnel permettra, étape par étape, de garantir que la protection des données soit satisfaisante et se maintienne sur le long terme.

[5] Licéité du traitement, loyauté et transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité et confidentialité, responsabilité.

Le RGPD peut être vu comme une opportunité ; celle d'améliorer l'organisation et les services. Ainsi, des outils, tels le registre de traitement et les analyses d'impact, s'ils sont pensés, construits et remplis pour servir le métier lui-même et pour faciliter le fonctionnement de l'institution ont beaucoup plus de chance d'être utilisés par les acteurs et mis à jour que des outils dédiés uniquement à la conformité RGPD.

Cette approche pragmatique permet également une plus grande maîtrise des coûts, qui ne sont dès lors plus uniquement imputables au RGPD lui-même, mais à l'augmentation de la qualité au sein de l'organisation.

Une question à garder à l'esprit au long de tout le processus : à quoi sert d'avoir de belles procédures si les personnes ne sont pas dans les conditions pour pouvoir les appliquer ?